UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Two cellular telephones described in Attachment A and currently at the U.S. Department of Homeland Security Office in Milwaukee, WI

Case No. 20 MJ 180

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Sections 2252A(a)(2)(A) & (b)(1), and 2252A(a)(5)(B) & (b)(2)	Distribution and possession of child pornography

The application is based on these facts:

See attached affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Nathan A Cravatta

Applicant's signature

HSI Special Agent Nathan A. Cravatta

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means).*

Date: August 14, 2020

William E. Duffin

Judge's signature

City and state: Milwaukee, WI

Hon. William E. Duffin, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Nathan A. Cravatta, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations (HSI), an investigative branch of the United States Department of Homeland Security. I am a federal law enforcement officer authorized by the Secretary of Homeland Security to request the issuance of criminal complaints and search warrants. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have been employed as a Special Agent with HSI since May 2005. I am currently assigned to the Resident Agent in Charge Office in Milwaukee, Wisconsin.

3. My experience as an HSI agent has included the investigation of cases involving the use of computers and the Internet to commit violations of federal law involving child exploitation, including the production, transportation, receipt, distribution and possession of child pornography. I have received training and have gained experience in interviewing and interrogation techniques, arrest procedures,

search warrant applications and the execution of searches, and seizures involving computer crimes. I have investigated and assisted in the investigation of criminal matters involving the sexual exploitation of children which constituted violations of Title 18, United States Code, Sections 2251, 2252 and 2252A.

4. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence, contraband, fruits and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252 and 2252A, incorporated herein by reference as if fully set forth, are located in the Devices for which authority is requested to search. Where statements of others are set forth in this affidavit, they are set forth in substance and in part.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The property to be searched is as follows (collectively, "Devices"):

   a. a Samsung Galaxy Model SM-J337P cellular phone, IMEI 352938091181177;

   b. a Google Pixel 3 XL cellular telephone, IMEI 990015226779

6. The Devices are currently located at the U.S. Department of Homeland Security-Homeland Security Investigations evidence locker located at 790 North Milwaukee Street, #600, Milwaukee, Wisconsin 53202.

7. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

8. The purpose of this application is to seize evidence of violations of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (distribution of child pornography); and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography).

KIK MESSENGER

9. Kik Messenger ("Kik") is designed for mobile chatting or messaging. To use this application, a user downloads the application to a mobile phone or other mobile device via a service such as Google Play Store, Apple iTunes, or another similar provider. Once downloaded and installed, the user is prompted to create an account and username. The user also has a display name, which is what other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature, and the two parties can then send each other messages, images, and videos.

10. Once downloaded and installed, the user also has a display name, which will be what other users initially see when transmitting messages back and forth. As part of the account creation process, Kik users are asked to supply a valid e-mail address, create a password, provide an optional date of birth, and user location. The user also has the option of uploading a "profile avatar" that is seen by others. Once the

Kik user has created an account, the user is able to locate other users via a search feature. The search feature usually requires the user to know the intended recipient's username. Once another user is located or identified, Kik users can send messages, images, and videos between two parties.

11. Kik also allows users to create chat rooms, of up to 50 people, to communicate in a group setting and exchange images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, Kik users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a "hashtag" that is easily identifiable or searchable by keyword.

12. Kik users frequently advertise their Kik usernames on various social networking sites in order to meet and connect with other users. In some cases, Kik also provides various avenues, such as dating sites and social media applications, for meeting other users. HSI undercover agents observed in some chats that many of the users stated they felt safe using Kik as a means of trading child pornography and for other illegal activities, due to the fact that Kik, until recently, is a Canadian based company, and not subject to the same United States laws. HSI undercover agents have noted messages posted in Kik chat rooms relating to the enforcement, deletion, or banning of users and rooms by Kik for the purpose of exchanging or distributing child pornography. HSI agents noted the comments to include the continued creation of new rooms and new user accounts to circumvent Kik's enforcement efforts.

SUMMARY OF INVESTIGATION INVOLVING KIK

13. In December 2019, HSI Milwaukee received an investigative referral from HSI's Cyber Crimes Center (C3) indicating that on June 12, 2019 at 2:02:02 p.m. Central Time, Kik Messenger user "tom12345xx" distributed one image which depicts child exploitation material using Kik. Kik reported the hash value of the distributed image matched their internal hash matching system of a known child exploitation image hash value[1]. I have reviewed this image and determined it depicts a child engaged in sexually explicit conduct. This image depicts the naked, lower torso area of a prepubescent female. The female's legs are raised, spread and slightly visible in the image. The female's vaginal area and buttock are visible in the image. A clear, white substance is visible in the vaginal area of the female which is the focal point of this image. The hand of an adult is placed on the left, upper thigh area of the female. Three fingers of the adult are also visible near the right, upper thigh area of the female. A pink colored blanket is placed underneath the buttock area of the female.

14. According to information provided by Kik, this image was uploaded from Internet Protocol (IP) address 47.34.34.78 which resolves to Charter Communications. The display name associated with this account is noted as being, "Tom M." The confirmed email account listed for this account is tm637036@gmail.com. The account

[1] Kik developed an internal hash matching system with a database of approximately 1.7 million known child exploitation image hash values. This system ran a hash value check against all images sent within Kik. When a user sent an image with a hash value that matched a child exploitation hash value in the database, the account is banned, and law enforcement is notified.

was registered on May 30, 2019 from Android device, SM-J337P. I have reviewed the IP logins into this account and determined from May 30, 2019 until June 12, 2019, logins occurred consistently from IP address 47.34.34.78.

15. On or about December 11, 2019, a Department of Homeland Security (DHS) summons was issued to Charter Communications requesting subscriber information for IP address 47.34.34.78 on the date and time "tom12345xx" uploaded and shared the image on Kik's chat platform.

16. On January 22, 2020, I received the requested records from Charter Communications. I have reviewed the information subsequently provided by Charter Communications and saw the IP address was assigned to Thomas METZ at 150 N. Main St., West Bend, Wisconsin 53095.

17. On March 19, 2020, information was received from the Wisconsin Department of Justice, Division of Criminal Investigation (DCI) regarding Thomas METZ. According to information received by DCI from the Wisconsin Department of Corrections (DOC), Sex Offender Registry Program (SORP) which I have reviewed, on December 31, 2019, METZ completed a sex offender registration form indicating he resided at 150 N. Main Street, #4, West Bend, Wisconsin 53095. A phone number provided by METZ is listed as (262) 365-4394.

18. On April 27, 2020, a subpoena was issued to Google LLC requesting records related to account tm637036@gmail.com, the confirmed email account associated with Kik user "tom12345xx." Records subsequently received from Google

LLC indicate email account tm637036@gmail.com was created on May 30, 2019. The name listed for this account is "Tom M." The last login into this account occurred on June 30, 2019. A recovery short message service (SMS) and sign in phone number provided for this account is listed as being "+12623654394."

PRIOR CONVICTION OF THOMAS METZ FOR 2ND DEGREE SEXUAL ASSAULT OF A CHILD UNDER 16 YEARS OF AGE

19. I have reviewed a Criminal Complaint (Case No. 2009CF000834) from Winnebago County, Wisconsin. According to this criminal complaint, on August 26, 2009, the Oshkosh Police Department received a report regarding the sexual assault of an eleven year old female. The minor female reported on August 25, 2009, that Thomas METZ, her mother's cousin who was residing with them, came into her bedroom, took his hand, and rubbed her under her underwear. METZ was later interviewed and asked if he ever touched the minor female inappropriately. METZ responded, "not that I meant to."

20. On May 10, 2010, Thomas J. METZ was found guilty by a jury in Winnebago County Circuit Court of 2nd Degree Sexual Assault of a Child. He was later sentenced to five years in prison followed by five years of extended supervision

21. Thomas METZ was on probation for a Burglary offense when he committed the aforementioned offense. His probation supervision was revoked. METZ was released from prison on October 9, 2018.

EXECUTION OF A SEARCH WARRANT AND SUBSEQUENT INTERVIEW OF THOMAS J. METZ

22. On July 30, 2020, officers and agents with HSI, DCI, and West Bend Police Department executed a search warrant at 150 N. Main Street, Apartment 4, West Bend, Wisconsin. A subsequent search of the residence resulted in the seizure of a cellular telephone, an Amazon Fire tablet, MP3 player, several compact disks, and a document reflecting indicia of occupancy. Forensic examinations will be conducted on all seized items.

23. During the execution of the search warrant, agents and officers located Thomas METZ. METZ agreed to speak to law enforcement. During this interview, METZ acknowledged he had used Kik approximately one year ago and it was possible his username was "tom12345xx." While using Kik Messenger, METZ recalled receiving and viewing images which depicted child exploitation material on approximately twenty occasions. He recalled some of these images depicted toddlers and infants. METZ also acknowledged he masturbated while viewing child pornography images he received on Kik.

24. METZ indicated he used a Google Pixel cellular telephone to access Kik. He stated this device, in addition a Samsung Galaxy cellular telephone (the "Devices"), were located at his mother's residence in West Bend, Wisconsin. He explained he turned the Devices over to his mother as a condition of his supervision. METZ signed a written consent to search form allowing law enforcement to search the Devices. METZ provided the password for both Devices.

25. On this date, law enforcement accompanied METZ to his mother's residence in West Bend, Wisconsin. While at the residence, METZ's mother, Debra Metz, voluntarily turned over the Devices to law enforcement. She also signed a written consent to search form.

TECHNICAL TERMS

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can

contain any digital data, including data unrelated to photographs or videos.

c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

d. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

e. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

27. Based on my training, experience, and research, and from consulting the manufacturers' advertisements and product technical specifications available online at https://www.samsung.com/us/business/support/owners/product/galaxy-j3-achieve-Sprint/ and https://pixel3xluserguide.com, I know that the Samsung Galaxy Model SM-J337P and Google Pixel 3 XL cellular telephones have capabilities that allow them to serve all or some of the following functions: wireless telephone, a digital camera, GPS navigation device, and accessing /downloading information from the Internet. In my training and experience, examining data stored on devices of these types can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

28. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

29. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

30. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

31. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

32. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

ATTACHMENT A

The property to be searched are as follows:

a. a Samsung Galaxy Model SM-J337P cellular phone, IMEI 352938091181177;
b. a Google Pixel 3 XL cellular telephone, IMEI 990015226779

The Devices are currently located at the U.S. Department of Homeland Security-Homeland Security Investigations evidence locker located at 790 North Milwaukee Street, #600, Milwaukee, Wisconsin 53202.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 18 USC 2251, 2252 and 2252A, including:

   a. Records containing child pornography or pertaining to the production, distribution, receipt, or possession of child pornography;

   b. Records or information, photographs, videos, notes, documents, or correspondence, in any format or medium, concerning communications about child pornography or sexual activity with or sexual interest in minors;

2. All names, aliases, and numbers stored in the Devices, including numbers associated with the Devices, relating to the identities of those engaged in the production, possession, receipt, or distribution of child pornography.

3. Images or visual depictions of child pornography.

4. Records and information containing child erotica, including texts, images and visual depictions of child erotica.

5. Any and all information, notes, software, documents, records, or correspondence, in any format and medium, pertaining to the violations.

6. Any and all address books, names, and lists of names and addresses of individuals who may have been contacted by use of the computer or by other means for the purpose of committing the violations.

7. The list of all telephone calls made or received located in the memory of the Devices that provides information regarding the identities of and the methods and means of operation and communication by those engaged in the possession, receipt, or distribution of child pornography.

8. Any and all information, notes, documents, records, or correspondence, in any format or medium, concerning membership in online groups, clubs, or services that provide or make accessible child pornography

9. Any and all information, records, documents, invoices and materials, in any format or medium, that concern e-mail accounts, online storage, or other remote computer storage pertaining to the violations.

10. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.